REMARKS

I. INTRODUCTION

In response to the Office Action dated October 6, 2003, claims 3, 16, 17, 32, 33, 47, 48, 55, 78, 79, 88 have been cancelled, claims 1, 4, 5, 18, 19, 35, 54, 56, 61, 71, 77, and 86 have been amended. Claims 1, 2, 4-15, 18-31, 34-46, 49-54, 56-77, 80-87, and 89 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. CLAIM AMENDMENTS

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for purposes of patentability.

III. OFFICE ACTION OBJECTIONS

In the Applicants' form 1449, the Examiner noted "need English" in connection with the recitation of document number EP 0 791 877 A1, but did not indicate that the reference was not considered. Pursuant to M.P.E.P. § 709, the Applicants state that this reference is considered "relevant" solely because it was cited the search report of the related PCT application. To assist the Examiner, however, the Applicants also hereby submit an equivalent version of the reference (EP 0 791 877 B1), which includes an English translation of the claims, and a machine-translated version of the text of the EP 0 791 877 B1 reference.

IV. THE CITED REFERENCES AND THE SUBJECT INVENTION

A. The Rallis Reference

U.S. Patent No. 6,425,084, issued July 23, 2002 to Rallis et al. disclose a notebook security system using infrared key that prevents unauthorized use of a computer. A program resident on the computer implements a user-validation procedure. An IR key device carries a first serial number and an encryption key. A second serial number corresponds to a device internal to the computer. A mass storage device installed in the computer stores a validation record that includes an unencrypted portion and an encrypted portion, the unencrypted portion including a copy of the first serial number and the encrypted portion including a

copy of said second serial number and a user personal identification number. The key device is coupled and interfaced with an infrared port on the computer by the user. The first serial number and the encryption key are read from the key device in order to gain authorized use of the computer. The key device may be decoupled from the computer after authorized use of the computer has been gained, and during operation of the computer.

B. The Subject Invention

The Applicants' invention is a compact, self-contained, personal key that permits storage of sensitive private user data, and prevents this data from being provided to the host computer without affirmative user authorization. The personal key comprises a processor which provides the host processing device conditional access to data storable in the memory as well as the functionality required to manage files stored in the personal key and for performing computations based on the data in the files. In one embodiment, the personal key also comprises an integral user input device and an integral user output device. The input and output devices communicate with the processor by communication paths which are independent from the USB-compliant interface, and thus allow the user to communicate with the processor without manifesting any private information external to the personal key.

C. Differences Between the Subject Invention and the Cited References

The Rallis reference is directed to a key that is used to prevent unauthorized use of a notebook computer. When the notebook is powered up, the user is prompted to connect a key to one of the available input ports (a USB port, a PS/2 port, or an IrDA port). If the proper key is coupled to the port, the notebook uses data provided by the key and an optional PIN entered into the notebook to unlock the notebook computer.

The Applicants' invention, as described in the above claims, is not directed to preventing unauthorized access to a host computer. Instead, it is directed to the storage and retrieval of user sensitive data, and to protecting this data so that the data is not provided to the host computer or anywhere else unless the token receives an affirmative input authorizing the token to provide the data. The Rallis "key" does not store user private data such as passwords and the like ... it stores a serial number and an encryption key, both of which are set by the manufacturer:

> The key device serial number and encryption key, usually a large prime number, are loaded into the key device 20 by the manufacturer.(col. 3, lines 27-29)

In the many embodiments described and claimed, the Applicants' invention provides for an integrated user input device for accepting the user input authorizing access to the sensitive data (thus preventing tampering), and an integrated user output device, which signals that access to the sensitive user data stored in the token is being requested and prompts the user to authorize such access.

The Rallis reference does not disclose a user input device signaling authorization of a processor operation authorizing access to the sensitive user data. When the Rallis key is coupled to the notebook, the serial number and encryption key are exchanged, no user authorization is necessary and no user authorization is performed.

The Rallis reference also does not disclose that this user input device is communicatively coupled to the token's processor by a path distinct from the USB-compliant interface. The only user input devices that are arguably coupled to the token's processor using a path distinct from the USB-compliant interface are the fingerprint sensor 28 and a transmit switch. The fingerprint sensor 28, however is not used to signal authorization of access to the user's sensitive information. Instead, the fingerprint sensor simply reads fingerprint data and provides that data to the notebook computer for processing and comparison. Likewise, the transmit switch does not signal authorization of access to the user's sensitive information. At best, it simply saves power so that the key's IR circuits are not activated until the stored serial number and encryption key is required to be transmitted to the notebook computer. Further, the depression of the switch is not in response to a message received in the token from the host processing device via the USB-compliant interface invoking the processor operation.

Finally, different embodiments of the Applicants' invention include the use of an integral user output device signaling that access to the user's sensitive data is required. This prevents the user from unknowingly providing access to such information, and serves as a prompt for the user to use the input device described above to signal authorization of such access. With these important differences in mind, please consider the Applicants' remarks below.

V. OFFICE ACTION PRIOR ART REJECTIONS

In paragraphs (1)-(2), the Office Action rejected claims 1-9, 13-25, 29-40, 44-50, 53-57, 60-63, 65-67, and 71-89 under 35 U.S.C. § 102(e) as unpatentable over "Rallis" (which "Rallis" reference is unclear, as addressed below). The Applicants respectfully traverse these rejections.

At the outset the Applicants note that the Office Action's form PTO-892 recites three patents that are issued to Rallis et al., including U.S. Patent 6,425,084, U.S. Patent 6,189,099, and U.S. Patent No. 6,401,205. Unfortunately, the Office Action does not indicate which of the three "Rallis" references is relied upon in rejecting the Applicants' claims. As far as the Applicants can ascertain, the reference that best correlates with the Office Action's arguments is U.S. Patent 6,425,084. The Applicants have therefore addressed their comments accordingly. Should the Examiner have intended to reference a different "Rallis" reference than that which is addressed herein by the Applicants, the Examiner is invited to contact the Applicants' attorney, Victor G. Cooper, directly to discuss the patentability of the Applicants' claims in view of the Rallis references.

With Respect to Claim 1: Claim 1 recites:

"A compact personal token, comprising ... a user input device, communicatively coupled to the processor by a path distinct from the USB-compliant interface, for accepting an input...".

According to the Office Action, the foregoing features are disclosed in the Rallis reference as follows:

> A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user. (col. 2, lines 62-67).

and in FIG. 1A, as reproduced below:

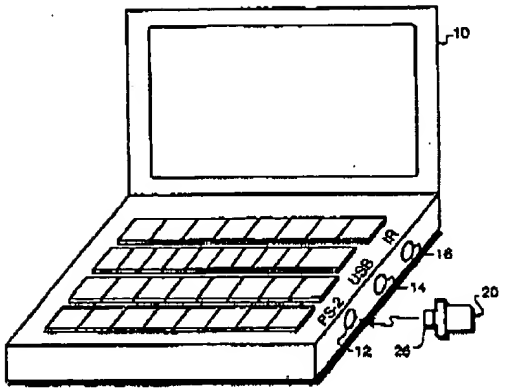

FIG. 1A

The Applicants respectfully disagree. The foregoing portions of the Rallis reference appear to disclose little more than a user-validation procedure, and Rallis itself expressly teaches a "key device" that has "no external controls" (see. col. 2, lines 46-47).

The Rallis reference does disclose a fingerprint reader 28, which reads fingerprint data and provides the data to the notebook for processing instead of the serial number and encryption key data:

> As an alternative to serial number and encryption key data, the key device 20 can include special security features, such as a finger print-reader 28 (FIG. 5C), or a "smartcard" reader that senses data on a "smartcard" 29 (FIG. 5D), to generate key data. This data is forwarded by the key device 20 to the user-validation program in a manner identical to the transmission of serial number and encryption key data. (col. 5, lines 14-21).

and also discloses an IR embodiment which uses a switch depression to transmit the key serial number and encryption key (presumably, to conserve key power):

> When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA). (col. 5, lines 51-57)

However, claim 1 recites that the accepted user input is *"for processing by the processor to signal authorization of a processor operation providing access to the user private data"* and that the input is provided *"in response to a message received in the token from the host processing device via the USB-compliant interface invoking the processor operation"*. Rallis teaches that the fingerprint data is transmitted to the notebook for processing instead of performing the processing in the token processor. Fingerprint input likewise does not signal authorization of a processor

operation providing access to user private data ... the fingerprint data is simply transmitted to the notebook computer. And neither fingerprint data nor the depression of the transmit switch is provided in response to a message received in the token from the host processing device via the USB-compliant interface." For all of these reasons, the Applicants respectfully traverse the rejection of claim 1.

With Respect to Claims 18-19: Claim 18 recites the step of:

"processing the user input in the processor to authorize the processor operation"

The Applicants traverse this rejection, because as pointed out above with respect to claim 1, nothing in the Rallis reference teaches (1) accepting a command in the token invoking a processor operation via a USB interface, (2) accepting a user input signaling authorization of that operation and providing the user input to a processor via a path distinct from the USB-compliant interface, and processing the user input in processor to authorize the invoked token processor operation.

Claim 19 recites the features of claim 18 and is patentable on the same basis. Claim 19 also recites features rendering it even more remote from the Rallis reference. Rallis, for example, does not disclose determining if a processor (token processor) requires access to private data stored in the token, and prompting the user to authorize the operation via an output device. The Office Action indicates that "access to private data is secured, because only the authorized user with the Pin can access the host computer system", but claim 19 recites that the process requires access to the private data *stored in the token*, not in the host computer.

With Respect to Claim 35: Claim 35 recites the steps of:

accepting a command in the token invoking a processor operation via the USB-compliant interface;

determining, in the token, if the processor operation requires access to the private data stored in the token;

prompting the user to authorize the processor operation via an output device communicatively coupled to the processor by a path distinct from the USB-compliant interface if the processor operation requires access to a private data stored in a memory in the token;

accepting a user input signaling authorization of the processor operation via an input device; and

providing the user input to the processor via a communication path distinct from the USB-compliant interface

The Rallis reference does not disclose accepting a command in the token invoking a processor operation via a USB-compliant interface, or determining, in the token, if the

processor operation requires access to the private data stored in the token. The Rallis reference likewise does not disclose accepting user input via a communication path distinct from the USB-compliant interface. Accordingly, the Applicants respectfully traverse the rejection of claim 35.

With Respect to Claim 49: Claim 49 recites a token having a processor for providing the host processing device conditional access to store and retrieve data storable in the memory, the data including personal identification private to the user, and a user input device, communicatively coupled to the processor by a path distinct from the USB-compliant interface, for accepting a user input describing the personal identification.

The fingerprint embodiment of the Rallis reference reads the user's fingerprint and provides that fingerprint data from the key 20 to the notebook computer for processing. No conditional access is provided ... Rallis teaches that the personal information is provided when the person grabs the key. The transmit switch does not accept user input *describing the personal identification.* For the foregoing reasons, the Applicants respectfully traverse the rejection of claim 49.

With Respect to Claims 54-55: Claim 54 recites the steps of:

determining if the processor operation requires access to the personal identification storable in a memory of the token; and

determining if the personal identification is stored in the memory of the token; and

prompting the user to enter a personal identification if the processor operation requires access to the personal identification and the personal identification is not stored in the memory of the token ...

The Rallis reference does not teach any of these forgoing features. Rallis simply provides a serial number or an encryption key (or in an alternative embodiment, fingerprint data) to the notebook for further processing. Further, while Rallis teaches prompting the user to connect the key:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. (col. 1, lines 59-64)

> A flow diagram of the user-validation procedure is shown in FIG. 3. In Step 1, the user-validation program prompts the user to attach the key device 20 to the notebook computer 10. The program attempts to communicate with the key device 20 for a fixed delay period. If a key device 20 is not detected within this period, then the program proceeds to Step 11 where the computer is automatically powered down. In Step 2, the program reads the key device serial number and encryption key that are stored in the key-device ROM 24. The key device serial number and encryption key, usually a large prime number, are loaded into the key device 20 by the manufacturer. (col. 3, lines 17-28)

teaches prompting the user to enter a PIN;

> In Step5, the user-validation program prompts the user to enter a PIN. The PIN consists of a string of six to eight characters. In Step 6, the program compares the PIN to the corresponding number stored in field 2 of the decrypted validation record. If the numbers do not match, the program moves to Step 11. If the system is configured to operate without the manual entry of a password or PIN, Steps 5 and 6 are bypassed. (col. 4, lines 13-20)

and teaches prompting the user to position an IR key device with the IR port of the notebook:

> When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA). (col. 5, lines 51-57)
>
> After the user-validation program prompts the user to align the IR key device 21 with the IR port 16, it transmits a command message containing a "super key" access code number. (col. 6, lines 10-13)

However, the Rallis reference does not teach determining if personal identification is required, if personal identification is stored in the token, and if it is not, prompting the user to enter the personal identification. Accordingly, the Applicants respectfully traverse the rejection of claim 54.

With Respect to Claims 61 and 71: Claim 61 recites that the user input device signals authorization of a processor operation. As described above, the "user input" data of the Rallis reference is fingerprint data that is simply forwarded to the notebook computer for further processing. The fingerprint data is not used to authorize a processor operation in the token itself. Claim 61 also recites that the user input device signals authorization of a processor operation invoked by a message received in the token via the USB-compliant interface. These features are likewise not disclosed in the Rallis reference.

Claim 71 recites the step of accepting "a user input to *control* the processor operation via an input device." The Rallis "user input" (fingerprint data) does not control the operation of the key's processor. Instead, the data is simply read and provided to the notebook computer for analysis. Further, the depression of the transmit switch does not *control* a processor operation invoked by a command accepted in the token via the USB-compliant interface. In fact, the Rallis reference itself teaches a key with *no external controls.* (see col. 2, lines 46-48). Accordingly, the Applicants respectfully traverse the rejection of claim 71.

With Respect to Claim 77: Claim 77 recites token having a user output device for providing an indication of a data signal from the USB-compliant interface. Nothing in the Rallis reference discloses this limitation. Accordingly, the Applicants respectfully traverse this rejection

With Respect to Claim 80: Claim 80 recites a compact personal token comprising a user output device. The "key" disclosed in the Rallis reference does not include a user output device. Accordingly, claim 80 are allowable over the Rallis reference.

With Respect to Claim 2, 23, and 38: Claims 2, 23, and 38 recite the features of independent claims 1 , 18, and 35, respectively and are patentable for the same reasons. Claim 23 also recites the features of claims 19 and 20 (discussed further below) and is patentable for those reasons as well.

With Respect to Claims 9 and 19: Claim 9 recites the features of claim 7 (including an output device communicatively coupled to the processor by a second path distinct from the USB-compliant interface). The Rallis reference fails to disclose such an output device and is patentable on this basis alone.

Claim 19 recites that the user is prompted to authorize the processor operation if the operation requires access to private data stored in the memory. As described above, Rallis fails to disclose these features.

With Respect to Claim 4: Claim 4 recites that the user private data is designated as requiring authorization before access by an associated identification stored in the token's memory. According to the Office Action, the foregoing features is disclosed as follows:

> The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. (col. 1, lines 62-67)

and

> A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user. (col. 2, lines 62-66)

The Applicants respectfully disagree that the foregoing discloses designating anything analogous to private data as requiring authorization before access by the token's processor.

With Respect to Claims 5, 24, 39, 53, 60, 65, and 73: Claims 5, 24, 39, and 73 recite the features of the claims they depend upon, and are patentable for the same reasons. Claims 53 and 60 recites two pressure sensitive devices actuatable from the exterior side of the token. According to the Office Action, this is disclosed as follows:

> Ideally, the IR key device 21 is of such shape and size as to be placed on the user's key chain. It is self-powered and in its basic configuration, as shown in FIG. 6B, includes an IR transmitter 27 and a momentary transmit switch 25, in addition to a microprocessor and ROM (not shown). (col. 5, lines 46-50)

Plainly, two pressure sensitive devices are not disclosed, and hence, claims 53 and 60 are allowable over Rallis.

With Respect to Claims 6, 25, 40, and 66: Claims 6, 25, 40, and 66 recite the features of the claims they depend upon and are patentable for the same reasons.

With Respect to Claims 7, 56, 74, and 88: The portion of the Rallis reference relied upon by the Office Action:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device.
> (col. 1, line 60 through col. 2, line 7)

fails to disclose an output device communicatively coupled to the token processor by a path independent from the USB-compliant interface. Accordingly, the Applicants respectfully traverse the rejection of claim 7. Claim 88 is allowable for analogous reasons.

Claims 56 and 74 recite prompting the user to enter the personal identification number or control the processor operation via a path distinct from the USB-compliant interface." This features are also not disclosed in Rallis.

With Respect to Claims 8, 21, 36, and 75: Claim 8 recites that the input device and output devices paths are a common path. According to the Office Action, this is disclosed as follows:

> The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device. (col. 2, lines 3-10)

The Applicants respectfully disagree and therefore traverse this rejection. Claims 21, 36, and 75 recite analogous limitations and are patentable for the same reasons.

With Respect to Claims 13, 29, 44: Claim 13 recites that the output device provides an alphanumeric message. According to the Office Action, this feature is disclosed as follows:

> The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. (col. 1, lines 61-63)

However, the user prompt is performed by the notebook computer, which is not communicatively coupled by a second path distinct from the USB compliant interface as required by claim 7. Claims 29 and 44 are patentable for analogous reasons.

With Respect to Claims 14, 30, and 45: According to the Office Action, the Rallis reference discloses that the alphanumeric message identifies the processing operation at (col. 1, lines 64-67 and col. 2, lines 1-7. The Applicants can ascertain no such disclosure, and therefore traverse the rejection of these claims as well.

With Respect to Claims 15, 31, and 46: Claim 15 recites that the alphanumeric message recites a private key. According to the Office Action, this feature is disclosed in Rallis as follows:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device.
> (col. 1, line 60 through col. 2, line 7)

The foregoing does not disclose presenting an alphanumeric message reciting a private key. Accordingly, the Applicants traverse the rejection of claim 15. Claims 31 and 46 are patentable for analogous reasons.

With Respect to Claims 16-17, 32-33, and 47-48: Rallis discloses none of the features cited in the foregoing claims. However, claims 16-17, 32-33, and 47-48 have been canceled to streamline prosecution of the present application.

With Respect to Claim 20: The Office Action alleges that FIG. 1A above discloses an output device communicatively coupled to the token processor by a second communication path distinct from the USB-compliant interface. The Applicants respectfully disagree.

With Respect to Claims 22 and 37: The Office Action alleges that col. 1, lines 61 through col. 2, line 10 of the Rallis reference discloses steps describing if a token processor requires access to a private key stored in the token. The Applicants respectfully disagree and traverse this rejection.

With Respect to Claims 50 and 57: Claims 50 and 57 recite that the token include a user input device that is a character input device. This feature is not even remotely suggested by Rallis. Accordingly, the Applicants traverse this rejection as well.

With Respect to Claim 62: Claim 62 recites:

> *a processor, communicatively coupled to the memory and communicatively coupleable to the host processing device via the USB-compliant interface, the processor for providing the host processing device conditional access to user private data storable in the memory; and*
> *a user input device, communicatively coupled to the processor by a path distinct from the USB-compliant interface, the user input device for signaling authorization of a processor operation invoked by a message received in the token via the USB-compliant interface.*

For the reasons described above with respect to claim 1, the Applicants respectfully traverse this rejection.

With Respect to Claims 63, 72, 83, and 87: Claim 63 recites that the operation performed by the token processor is selected from the group comprising an encryption operation and a decryption operation. According to the Office Action, this is disclosed at col. 1, lies 1-10 of the Rallis reference. The Applicants respectfully disagree, as the "key" in the Rallis disclosure does not encrypt or decrypt anything ... it simply transmits encrypted information. The analysis with respect to claims 72, 83, and 87 is analogous.

With Respect to Claims 76, 84, and 89: Claim 74 recites that the output device is selected from the group comprising an LED, LCD, or an aural reproduction device. The Office Action indicates that these features have already been addressed, but the Applicants disagree. Plainly, the Rallis reference does not disclose a token having an LED, LCD, or an aural reproduction device. The analysis of claims 84 and 89 is analogous.

With Respect to Claims 56 and 81: Claim 56 recites that the step of prompting the user to enter the personal identification number comprises the step of activating a user output device via a second communication path distinct from the USB-compliant interface. The Office Action indicates that this is discloses as follows:

> In the "super key" configuration, the IR key device 21 includes both an IR transmitter and IR receiver, but does not include a transmit switch. The IR key device 21 remains the powered-down state until it receives an IR pulse. After the user-validation program prompts the user to align the IR key device 21 with the IR port 16, it transmits a command message containing a "super key" access code number. The access code procedure requires the IR key device 21 to verify receipt of a matching code number before it will output the serial number and encryption key data. Preferably, the access code "hops", or changes, each time the IR key device 21 is accessed. If the IR key device 21 is verifies a match between the received access code and a number stored within the device, it transmits a response message containing the key device serial number and the encryption key. (col. 6, lines 7-22).

The Applicants traverse this rejection. The foregoing does not disclose activating a user output device via a second communication path distinct from the USB-compliant interface. Claim 81 is allowable for analogous reasons.

With Respect to Claim 82: Claim 82 recites that the output device is configured to indicate the operation of the processor. As described above, this is not disclosed in the Rallis reference.

With Respect to Claims 67 and 85: Claims 67 and 85 are allowable for the same reasons as claim 82.

With Respect to Claim 86: Claim 86 recites:

> *A method of authorizing access to private data stored in a token having a processor communicatively coupled to a host processor via a Universal Serial Bus (USB) interface, comprising the steps of:*
>
> *accepting a command in the token invoking a processor operation via the USB-compliant interface; and*
>
> *signaling the processor operation via a user output device communicatively coupled to the processor via a communication path distinct from the USB-compliant interface..*

According to the Office Action, these features are disclosed as follows:

> The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. (col. 1, lines 62-67)

and

> A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user. (col. 2, lines 62-66)

However, nothing in Rallis discloses signaling a token processor operation (invoked by accepting a command in a USB-compliant interface) via a user output device communicatively coupled to the token processor via a communication path distinct from the USB-compliant interface. Accordingly, the Applicants respectfully traverse the rejection of claim 86 as well.

In paragraphs (28)-(29), the Office Action rejected claims 10-12, 26-28, 41-43, 51-52, 58-59, 64, and 68-70 under 35 U.S.C. §103(a) as being unpatentable over Rallis. Applicants respectfully traverse these rejections.

With Respect to Claims 10-12, 26-28, 41-43, and 68-70: Claim 10 recites that the user output device is a light emitting diode. The Office Action takes official notice that having a light emitting device is well known, "because it allows the user to know that activity is being performed on the device." However, whether LEDs are well known in the art or not, there is no teaching whatever in Rallis to add an output device at all, let alone use it to inform the user of activity performed on the device. Indeed, there is no reason why the user would want to know what activity is being performed in the key ... the Rallis "key" is simply used to unlock the notebook computer. Accordingly, the Applicants traverse the rejection of claim 10 as well as the "official notice" taken in rejecting this claim.

Claims 26, 41, and 68 recite analogous features and are patentable for the same reasons.

Claims 11, 27, 42, and 70 recite an aural device, and are patentable for the same reasons.

Claims 12, 28, 43, and 69 recite an LCD display and are patentable for the same reasons.

With Respect to Claim 64: Claim 64 recites that the processor operation invoked by the message received in the token via the USB-compliant interface comprises a digital signature operation using a private key stored in the memory. According to the Office Action, that one of ordinary skill in the art would be motivated to use a digital signature operation since it would verify the sender.

The Applicants respectfully traverse this rejection. The Rallis reference discloses a system wherein a notebook computer is unlocked using a key matching a PIN stored in the notebook. This itself "verifies the sender", and nothing more is required. The Rallis reference itself teaches the use of the matching PIN for authentication, and hence, teaches away from the Applicants' invention. "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the Applicants. The degree of teaching away will of course depend on the particular facts; in general, a reference's disclosure will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the Applicant. *In re Gurley*, 27 F.3d 551, 553, 31 U.S.P.Q.2d 1130 (Fed. Cir. 1994). The Applicants therefore traverse the rejection of claim 64.

With Respect to Claims 51-52, and 58-59: The Office Action indicates that it would be obvious to have a character input device that includes a wheel and an input position for each character. However, Rallis teaches that the PIN is entered via the notebook computer. Further, the only input devices envisioned by the Rallis reference are a fingerprint sensor and a switch to turn the IR embodiment on and transmit the serial number and encrypted key data. A character input device would hardly be an obvious substitution for either of these devices. Accordingly, the Applicants respectfully traverse the rejection of these claims as well.

VI. DEPENDENT CLAIMS

Dependent claims 2-17, 19-34, 36-48, 50-53, 55-60, 62-70, 72-76, 78-79, 81-85, 87-89 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

VII. CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: January 6, 2004

By: _____
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/amb